Caleb Marker (SBN 269721)
Email: caleb.marker@zimmreed.com
ZIMMERMAN REED LLP
6420 Wilshire Blvd, Suite 1080
Los Angeles, CA 90048
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

Attorneys for Plaintiff
(additional attorneys listed on signature page)

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

KIMBERLY KINNEY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

POWERSCHOOL HOLDINGS, INC.,

Defendant.

Civil Action No.:

CLASS ACTION

CLASS ACTION COMPLAINT FOR:

1. **Negligence**
2. **Negligence per se**
3. **Breach of Implied Contract**
4. **Invasion of Privacy**
5. **Unjust Enrichment**
6. **Breach of Fiduciary Duty**
7. **Declaratory Judgment**

DEMAND FOR JURY TRIAL

Plaintiff Kimberly Kinney ("Plaintiff"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon the investigation of counsel, brings this class action against Defendant PowerSchool Holdings, Inc. ("PowerSchool" or "Defendant") for its failure to properly secure and safeguard Plaintiff's and/or Class Members' personally identifiable information stored within Defendant's information network (these types of information, *inter alia*, being thereafter referred to collectively as "personally identifiable information" or "PII"[1]). All such information is referred to in the aggregate herein as "Private

[1] PII generally incorporates information that can be used to distinguish of trace an individual's identity, either along or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individually. PII is also generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong (footnote continued)

Information."

SUMMARY OF ACTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused, and continues to cause, to Plaintiff and other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendant on December 28, 2024, by which cybercriminals infiltrated Defendant's inadequately protected network and accessed the Private Information which was being kept under-protected by Defendant (the "Data Breach").

2. While Defendant claims to have discovered the breach as early as December 28, 2024, Defendant did not begin informing victims on the Data Breach until January 7, 2025 and failed to inform victims when or for how long the Data Breach occurred. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received letters from Defendant informing them of it.

3. Defendant acquired, collected, and stored Plaintiff's and Class Members' Private Information. Therefore, at all relevant times, Defendant knew or should have known that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential Private Information.

4. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure the Plaintiff's and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

---

hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers, etc.).

5. Plaintiff and Class Members have a continuing interest in ensuring their information is and remains safe and are entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount of controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members. Plaintiff is a resident of a different state than Defendant.

7. This Court has personal jurisdiction over PowerSchool because it is headquartered in this district and conducts substantial business in this district. It has also conducted systematic and continuous activities in California; and there is a substantial nexus between the conduct PowerSchool directs at California and the claims asserted herein.

8. Venue is proper in this Court because Defendant is headquartered in this district.

PLAINTIFF

9. Plaintiff Kimberly Kinney is an adult individual and, at all relevant times herein, a resident and citizen of the State of Indiana. Plaintiff Kinney is a victim of the Data Breach.

10. Plaintiff Kinney is a teacher in the Brownsburg School Corporation, which uses PowerSchool products. As a result, she has provided her PII to PowerSchool. On or about January 8, 2025, Plaintiff Kinney received a breach notice from her school corporation, originally sent by PowerSchool, that her personal information was accessed in the Data Breach.[2]

11. Defendant received highly sensitive Private information from Plaintiff in connections with the services Defendant provided to Plaintiff. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

12. At all times herein relevant, Plaintiff is and was a member of the Class.

13. Plaintiff's Private Information were exposed in the Data Breach because Defendant stored and/or shared Plaintiff's Private Information.

[2] Exhibit A, Kimberly Kinney Notice of Security Incident (January 8, 2025)

14. Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

15. Plaintiff received a letter from Defendant stating that Plaintiff's respective Private Information was involved in the Data Breach (the "Notice").

16. As a result, Plaintiff spent time dealing with the consequences of the Data Breach, which included and continues to include, time spent verifying the legitimacy and impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring their respective accounts, and seeking legal counsel regarding Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has been lost forever and cannot be recaptured.

17. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised as a result of the Data Breach.

18. Plaintiff has suffered and continues to suffer lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have respectively had anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling Plaintiff's Private Information.

19. Plaintiff has also suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

20. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

DEFENDANT

21. PowerSchool is the largest provider of cloud-based education software for K-12 education in the U.S., serving more than 75% of students in North America.

22. PowerSchool's software is used by over 16,000 customers to support more than 50 million students in the United States.

23. PowerSchool offers a full range of services to help school districts operate, including platforms for enrollment, communication, attendance, staff management, learning systems, analytics, and finance.

24. Due to the nature of its business PowerSchool receives and maintains PII for millions of students, parents, and school faculty across the country. Under state and federal law, PowerSchool had a duty to protect the PII of current and former students and school faculty members, including under Section 5 of the Federal Trade Commission Act ("FTC Act"). It likewise had a duty to promptly alert the students, parents, and school faculty that their PII was accessed by an unauthorized third party and which PII was at issue.

25. In the Global Privacy Statement on its website, PowerSchool tells users it is "committed to protect [users'] personal information" and that it "endeavors to align its privacy and security operations to best practices and relevant international regulations." As alleged below, PowerSchool does no such thing.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here May currently be unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

27. PowerSchool is a Delaware corporation headquartered at 150 Parkshore Drive, Folsom, California 95630.

COMMON FACTUAL ALLEGATIONS

The Cyberattack

28. In the course of the Data Breach, one or more unauthorized third parties accessed Class Members' Private Information. Plaintiff was among the individuals whose data was accessed in the Data Breach.

29. According to the Data Breach Notification and/or publicly filed documents, Plaintiff states, on information and belief, that millions of persons were affected by the Data Breach.

30. Plaintiff was provided the information detailed above upon Plaintiff's receipt of a letter and/or electronic notice from Defendant. Plaintiff was not aware of the Data Breach until receiving that notice.

Defendant's Failed Response to the Data Breach

31. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' Private Information with the intent of misusing the Private Information, including marketing and selling Plaintiff's and Class Members' Private Information.

32. Ten days after it claims to have discovered the Data Breach, Defendant finally began sending the Notice to persons whose Private Information Defendant confirmed was potentially compromised as a result of the Data Breach. The Notice provided basic details of the Data Breach and Defendant's recommended next steps.

33. PowerSchool has acknowledged that the information accessed in the Data Breach included at the least the following:

i. Names;

ii. Addresses;

iii. Social security numbers;

iv. Phone numbers;

v. Email addresses;

vi. Medical information;

vii. Grades and grade point averages;

viii. Bus stops for students;

ix. Notes and alerts concerning students;

x. Student IDs; and

xi. PII of parents of guardians of students.

34. Plaintiff and Class Members were required to provide their Private Information to Defendant in order to receive services. Thus, Defendant created, collected, and stored Plaintiff's and Class Members' Private Information with the reasonable expectation and mutual understanding that

Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what specific data was stolen, the particular malware used and what steps are being taken, if any, to secure their Private Information going forward.

36. Plaintiff and Class Members are left to speculate as to where their Private Information ended up, who has used it, and for what potentially nefarious purposes. Indeed, they are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

37. Plaintiff's and Class Members' Private information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing with Plaintiff's and/or Class Members' approval. Either way, unauthorized individuals can now easily access Plaintiff's and Class Members' Private Information.

Defendant Collected/Stored Class Members' Private Information

38. Defendant acquired, collected, stored, and assured reasonable security over Plaintiff's and Class Members' Private Information.

39. As a condition of its relationship with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential Private Information. Defendant, in turn, stored that information on Defendant's system that was ultimately affected by the Data Breach.

40. By obtaining, collecting, and storing Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties over the Private Information and knew or should have known that it was thereafter responsible for protecting Plaintiff's and Class Members' Private information from unauthorized disclosure.

41. Plaintiff and Class Members have taken reasonable steps to maintain their Private Information's confidentiality. Plaintiff and Class Members relied on Defendant to keep their Private

Information confidential and securely maintained, to use this information for business purposes only and to only make authorized disclosures of this information.

42. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' Private information.

43. Defendant's negligence in safeguarding Plaintiff's and Class Members' Private Information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

44. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendant was and/or certainly should have been on notice and aware of such attacks occurring in its industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendant is a large, sophisticated operation with resources to put adequate data security protocols in place.

45. And yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

46. In failing to adequately secure Plaintiff's and Class Members' sensitive data, Defendant breached duties it owed Plaintiff and Class Members under statutory and common law.

47. Plaintiff and Class Members surrendered their highly sensitive Private Information to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also had an implied duty to safeguard their Private Information, independent of any statute.

48. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is

an "unfair practice" in violation of the FTC Act. *See, e.g. FTC v. Wyndham Worldwide Corp.,* 799 F.3d 246 (3d Cir. 2015).

49. In addition to its statutory obligations, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

50. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that all Private Information in its possession was adequately secured and protected.

51. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect all Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

52. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach of its data security systems in a timely manner.

53. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

54. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Private information from theft because such an inadequacy would be a material fact in the decision to entrust their Private Information to Defendant.

55. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probably victims of any inadequate security practices.

56. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

57. Indeed, central to its core business, PowerSchool collects highly personal data for tens of millions of students, parents, and school faculty. It generates hundreds of millions of dollars annually through the collection, storage, and use of this information. It therefore had ample resources and a strong motive to adopt reasonable protections. It also should have known that such protections were necessary given the highly personal nature and value of information it stores.

58. PowerSchool knew or should have known that it would almost certainly be the target of hackers. Similar education technology providers have been subject to data breaches in previous years. More recently, PowerSchool informed the FBI that it was subject to a campaign to obtain PowerSchool's data.

Value of the Private Information

59. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant's conduct in causing the Data Breach.

60. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

61. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[3]

[3] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited June 6, 2022).

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. Fraudulent attempt to open bank accounts in their names.

b. The loss of the opportunity to control how their Private Information is used.

c. The diminution in value of their Private Information.

d. The compromise and continuing publication of their Private Information.

e. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud.

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud.

g. Delay in receipt of tax refund monies.

h. Unauthorized use of stolen Private Information; and

i. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in their possession.

63. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[4]

64. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen

[4] *See* Here's How Much Your Private Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 6, 2022).

private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. Indeed, the high value of Private Information to criminals is evidenced by the prices they will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6] Criminals can also purchase access to entire company breaches from $999 to $4,995.[7]

66. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

67. One such example of criminals using PII for profit is the development of "Fullz" packages.[8]

---

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at:* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[6] *Here's How Much Your Personal Information is Selling for on the Dark Web,* Experian, Dec. 6, 2017, *available at:* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[7] *In the Dark,* VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[8] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited January 9, 2024).

68. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

69. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

70. Defendant disclosed the Private Information, PII and/or PHI, of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

71. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Private Information of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

72. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving

them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

73. Unfortunately, there may be a lag time between when harm from a data breach occurs versus when it is discovered and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

74. When cybercriminals access financial information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may have exposed Plaintiff and Class Members.

75. And data breaches are preventable.[10] As Lucy Thompson wrote in Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by the proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[11]

76. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.[12] Here, Defendant's lax security and failure to create or

---

[9] *Report to Congressional Requesters,* GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf/

[10] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in Data Breach and Encryption Handbook* (Lucy Thompson, ed., 2012).

[11] *Id.*

[12] *Id.*

enforce these policies and procedures led to the Data Breach and harm to Plaintiff and Class Members.

77. Defendant knew of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if Plaintiff and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendant knew or should have known that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Its failure to do so is therefore intentional, willful, reckless, and/or grossly negligent.

78. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia,* (i) intentionally, willfully, recklessly and/or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

79. Following the Data Breach, PowerSchool is attempting to adopt and implement reasonable data systems and procedures. As it explained following the Data Breach, PowerSchool is now "Securing the Portal" that was used to access the data and "Strengthening Security" for its systems. But these measures are too late for Plaintiff and Class Members. PowerSchool should have implemented these reasonable measures before the Data Breach.

80. PowerSchool has done little to help those impacted by the Data Breach. It appears to have offered credit monitoring services to only some of its victims. These services do not compensate Plaintiff or Class Members for injuries sustained to date and, at most, provide limited protections moving forward.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this action pursuant to Rule 23(b)(2), 23(b)(3), and 23(b)(4) of the Federal Rules of Civil Procedure, on behalf of Plaintiff and the following class (collectively the "Class"):

"All individuals whose PII was exfiltrated or stolen in the Data Breach."

82. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for option out, any and all federal, state, or local governments, including, but not limited to, its departments, agencies, divisions, bebeerus, boards, sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

83. In the alternative, Plaintiff may request subclasses as necessary based, e.g., on the types of Private Information that were compromised.

84. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and the motion for class certification.

85. This action has been brought and may be properly maintained as a class action under Rule 23(b) because there is a well-defined community of interest in the litigation and membership in the proposed Class is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Membership in the Class will be determined by analysis of the Defendant's records.

b. Commonality: Plaintiff and Class Members share a community of interest in that there are numerous common questions and issue of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their Private Information;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

6) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

7) How and when Defendant learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Plaintiff's and Class Members' Private Information;

9) Whether defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

11) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of Plaintiff and Class Members inability to access the funds in their respective accounts and other services promised by Defendant;

12) Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective, and/or declaratory relief

and/or an account is/are appropriate as a result of Defendant's wrongful conduct; and

13) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that that Plaintiff has the same interest in the litigation of this case as the Class Members, are committed to vigorous prosecution of the case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each members makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual members of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impeded their ability to adequately protect their interests.

86. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

87. This class action is also appropriate for certification because defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

88. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinge on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

89. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

90. Finally, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

91. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

92. Plaintiff and the Class (or their third-party agents) entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

93. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

94. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

95. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probably class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class members' Private Information.

96. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. Exercise reasonable care in handling and using the Private Information in its care and custody;

b. Implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. Promptly detect attempts and unauthorized access;

d. Notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their Private Information.

97. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

98. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

99. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

100. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class (or their third-party agents) entrusted Defendant with their confidential Private Information, a necessary party of obtaining services from Defendant.

101. The risk that unauthorized persons would attempt to gain access to Private Information, and misuse it, was foreseeable by Defendant. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

102. Private Information is highly valuable, and Defendant knew, or should have known, that the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

103. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

104. Defendant breached these duties as evidenced by the Data Breach.

105. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' Private Information by:

a. Disclosing and providing access to this information to third parties; and

b. Failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

106. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff's and Class members' injury.

107. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class members' injuries-in-fact.

108. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

109. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff, and Class members have suffered, continue to suffer, or will suffer damage,

including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

110. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

111. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

112. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Class members' actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, lost access to their banking accounts; and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which Plaintiff and Class members continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

113. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

114. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

115. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class members' sensitive PII/PHI.

116. Defendant breached its respective duties to Plaintiff's and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

117. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

118. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class members would not have been injured.

119. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

120. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

121. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

122. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

123. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

124. Plaintiff and Class members (or their third-party agents) were required to provide their PII/PHI to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class members (or their third-party agents) provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's services.

125. Plaintiff and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

126. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

127. Plaintiff and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for services.

128. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

129. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Members' PII/PHI.

130. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

131. After all, Plaintiff and Class members (or their third-party agents) would not have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

132. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

133. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In

short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

134. Defendant materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

135. In these and other ways, Defendant violated its duty of good faith and fair dealing.

136. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed supra).

137. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

138. Plaintiff and Class members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

139. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

140. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to its current and former customers, including Plaintiff and the Class (or their third-party agents), to keep this information confidential.

142. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII/PHI is highly offensive to a reasonable person.

143. The intrusion was into a place or thing which was private and entitled to be private.

144. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

145. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

146. Defendant acted with a knowing state of mind when it permitted the Data Breach 18 because it knew its information security practices were inadequate.

147. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

148. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

149. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

150. And, on information and belief, Plaintiff's PII/PHI has already been published— or will be published imminently—by cybercriminals on the Dark Web.

151. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

152. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

153. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

154. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

155. This claim is pleaded in the alternative to the breach of implied contract claim.

156. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI (and/or payment) to provide services.

157. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

158. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

159. Defendant enriched itself by saving the costs they reasonably should have 4 expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

160. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures.

Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

161. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' PII/PHI and/or payment because Defendant failed to adequately protect their PII/PHI.

162. Plaintiff and Class members have no adequate remedy at law.

163. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

164. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

165. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

167. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

168. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

169. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

170. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

172. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

173. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and still are—inadequate and unreasonable

174. Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

175. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

176. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

177. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

178. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages— while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class members' injuries.

179. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

180. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

181. Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class;

b. Appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

c. Awarding declaratory and other equitable relief as necessary to protect the interests of the Plaintiff and Class;

d. Awarding injunctive relief as necessary to protect the interests of the Plaintiff and the Class;

e. Enjoining Defendant from further unfair and/or deceptive practices;

f. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

g. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

h. Awarding attorney's fees and costs, as allowed by law;

i. Awarding prejudgment and post-judgment interest, as provided by law;

j. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

k. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Respectfully submitted,

Dated: January 9, 2025

/s/ Caleb Marker

Caleb Marker
ZIMMERMAN REED LLP
6420 Wilshire Blvd, Suite 1080
Los Angeles, CA 90048
Telephone: (877) 500-8780
Facsimile: (877) 500-8781
caleb.marker@zimmreed.com

JENNINGS & EARLEY PLLC
Christopher D. Jennings*
Tyler B. Ewigleben*
500 President Clinton Avenue, Suite 110
Little Rock, Arkansas 72201
Telephone: (501) 372-1300
chris@jefirm.com
tyler@jefirm.com

ZIMMERMAN REED LLP
Brian C. Gudmundson*
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com

* *Pro Hac Vice* applications to be submitted

Counsel for Plaintiff and the Proposed Class